Internet Voting in Estonia

Sven Heiberg

Cybernetica AS

I-Voting in Estonia

- I-Voting success-story so far
  - 2005, Local government, **9 317** (0.9% / 1.9%)
  - 2007, Parliament, **30 275** (3,4% / 5,5%)
  - 2009, European Parliament, **58 669** (6,5% / 14,7%)
  - 2009, Local government, **104 413** (9,5% / 15,8%)
  - 2011, Parliament, **140 764** (15,4% / 24,3%)
- 2011, Parliament
  - 56% of advance voters were also i-voters
  - I-votes were sent out of 105 states

Criticism

- 06.09.2010, Swiss E-Voting Workshop, cryprographer Helger Lipmaa (Cybernetica AS) claims that Estonian solution has been insecure from the very beginning
- 09.03.2010, Pealtnägija, student Paavo Pihelgas claims that Estonian solution has been insecure from the very beginning and he has written a virus to prove it

Should we surrender?

- HL & PP have made some serious claims, they have strong point
- The story of Estonian i-Voting is a story about developing a multifaceted information system with complex requirements
- Security is relevant

The Constitution

- §1 – Estonia is independent and sovereign democratic republic. The supreme power is vested in the people.
- §56 – People exercise their power through citizens' right to vote.

Power

- Ability of an actor to realize his or her will in a social action, even against the will of other actors
- Election is process by which people delegate their power to small set of people
- Power can take many forms, it depends on the will of an actor in power
- Election is one of the legal means to gain certain kind of power

Electoral systems

- Electoral systems determine the means by which votes are translated into seats in the process of electing politicians into office
  - Single Member Plurality Systems
  - Majoritarian Systems
  - Proportional Systems
- How do you transfer 900 000 opinions into 101 seats so that everybody stays happy?

Voting methods

- Voting methods are there to support electoral systems – by voting methods ballots are gathered
- There should be enough voting methods to ensure that every citizen has access to elections in a way as it is stated in the Constitution
- Voting methods must be trusted by the general public – it does not suffice to be clean, it also has to look clean
- One must be able to observe

The Constitution revisited

- §1 – Estonia is independent and sovereign democratic republic. The supreme power is vested in the people.
- §56 – People exercise their power through citizens' right to vote.
- §156 – Local governments are elected in free elections for three years. Elections shall be general, uniform and direct. The ballot is secret.

Elections

- Elections are free
  - You decide how to vote
- Elections are general
  - All citizens have right to vote
- Elections are uniform
  - All votes are equal
- Elections are direct
  - The vote is given to candidate not party
- The ballot is secret
  - No-one has to know whether and how you voted

Interested parties

- Those actors who are interested in who has the power are interested in observing that the elections are held according to the law
- Some of those actors are ready to bend the law in order to achieve their way
- For some actors the bending of the law is the only way

Security is relevant

- To ensure correct functioning of the electoral system it is important to secure the voting methods, otherwise we cannot trust the ballots
- Security has several layers
  - Organizational
  - Physical
  - Technical
  - Scientific

P-voting protocol

- Voting in polling station
  - Voter gives his **identification** to election-official
  - Voter gets 1 piece of ballot paper
  - Voter gives **signature** to polling list
  - Voter goes inside voting booth and casts his vote in **privacy**
  - Voter puts ballot into the ballot box
- During counting no ballot can be traced back to voter

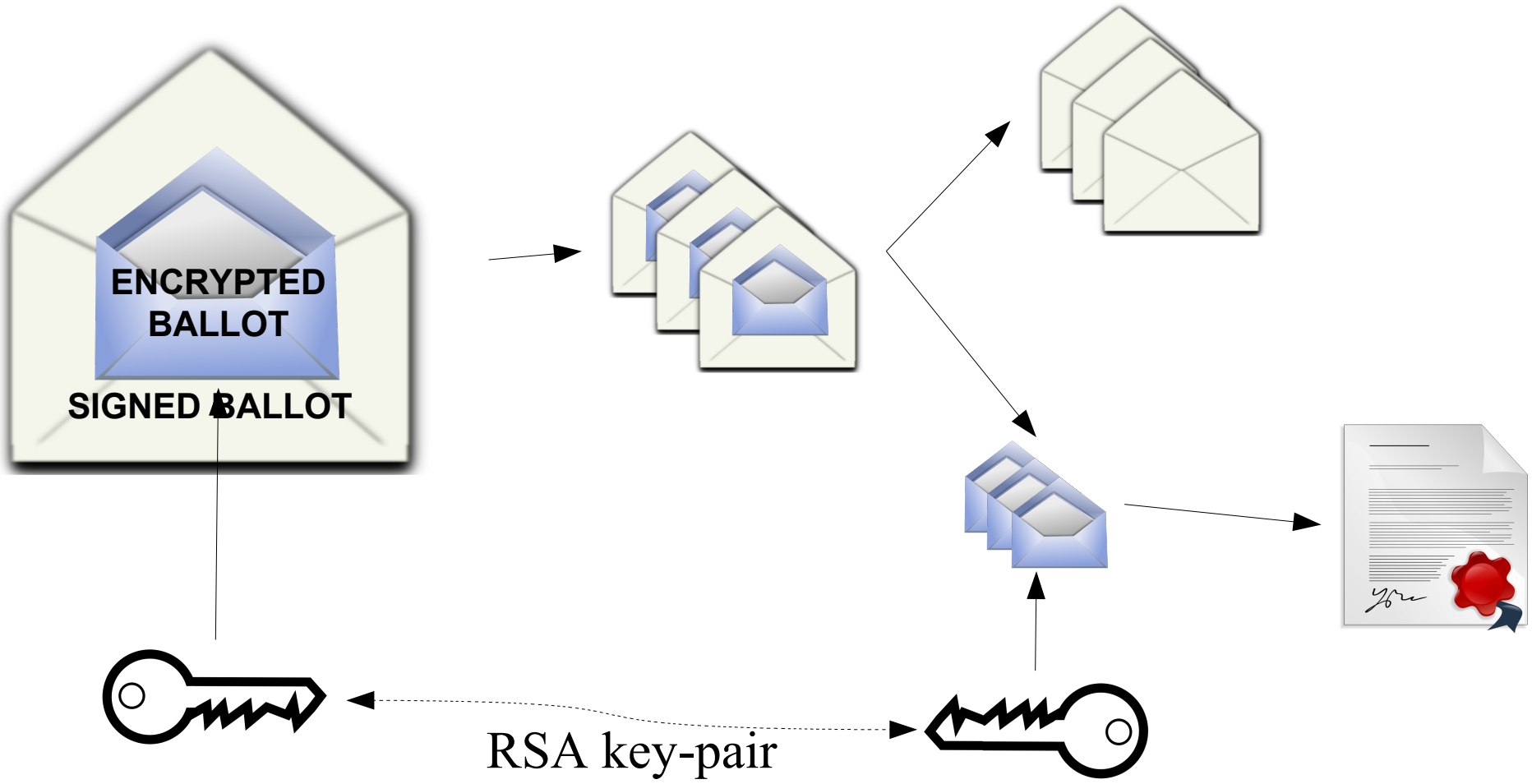
P-voting per post

- Voter receives 1 ballot paper and 2 envelopes
  - Candidate number is written on the ballot paper
  - Ballot paper is put inside first envelope
    - Nothing can be written on the envelope
  - The envelope is put inside second envelope
    - Second envelope has voter's personal identification and signature
- Counting occurs in 2 separated phases
  - Anonymization: outer envelopes are removed
  - Tabulation: inner envelopes are removed

I-voting protocol

- I-voting protocol resembles voting by post
  - Voter authenticates to voting server with ID-card
  - Voter encrypts his choice with server's public key
    - This is the first envelope
  - Voter digitally signs the encrypted ballot with ID-card
    - This is the second envelope
  - Digitally signed encrypted ballot is sent to voting server
- Counting again occurs in 2 separated phases

Vote Protection Protocol



What about coercion?

- P-voting takes place in voting booth
- I-voting can occur anywhere
  - Vote buying
  - Family voting
- I-vote revocation
  - P-vote takes precedence over i-vote
  - Several i-votes can be given, only last one will count
- What about uniform elections?

Components of I-Voting System

- Client software
  - UI, authentication, encryption, digital signature
- Server
  - Vote Forwarding Server (internet)
    - Authentication, candidate lists' distribution
  - Vote Storing Server (intranet)
    - Vote storage, anonymization
  - Vote Counting Server (offline)
    - Tabulation
- Auditing

Organizational Security

- Security of I-voting conception is not fully cryptographical/technical
  - Voters' identities have to be separated from plain votes
  - Software setup and maintenance must be made by authorized personell only
  - All stages of the process must be open to observers

The I-Voting is possible!

It's all about the manipulation

- Some kind of manipulation we accept
  - Campaign
  - Scandals
  - Threats and promises
- Some kind of manipulation we do not accept
  - Coercion
  - Vote buying
  - Tampering with results (directly/indirectly)
- Let's be evil for a minute

Think about the perfect crime

- What would be the reasons to attack i-voting system?
  - Fame? Power? Manipulation?
  - Political issues vs. financial issues
  - Is 99% of i-votes to some-party naive attack?
    - Riots in Tallinn would be good thing to...
    - i-voting is tool to manipulate election results
    - Not all parties are successful in i-voting
  - It would be good to have a hand on pulse...
    - Parliament is sometimes 200 votes away...

Attack types

- Real
  - Tampering with results
  - Breaking anonymity
  - Denial of Service
- Imaginary
  - For FUD it can be enough to present your way of thinking in Pealtnägija
  - Imaginary attacks can turn into reality
    - Revocation of results
    - Riots on the streets

Attackers

- Who?
  - Power, party, software developer, neighbouring state
- Why?
  - Stay in power, acquire power, vengeance, proof of skill, influence
- What was motivation for PP?
  - Developed his virus during demo-elections
  - Turned to media during real elections
  - Tried to revoke the results

Which door should I use?

- Server?
  - Tabulation application decides the parliament
  - How can voter say that his vote has been taken into account?
  - Org. and tech. security is high
  - One entry point
  - Trust is a bad thing
- Client?
  - Home computers' security is usually weak
  - Trojan can peek your vote
  - Trojan can change your vote without you noticing it
  - Distributed attack

Client side attacks

- Voter anonymity is lost cause?
- Possible ways to attack vote integrity
  - Modify the behaviour of original client
    - Change certain memory locations
    - Attack UI event-loop
  - Rouge application
    - Fake-UI
  - Non-UI protocol implementation
    - Intercept other ID-card uses

The problem

- Internet voting client application is our man in the enemy territory
- Internet voting server is base-camp
- How to make sure that the message we get from our scout
  - Comes from the legitimate application
  - Is unmodified

Is integrity protection possible?

- Zero-trust
  - If we cannot trust the computer, let's not give him the information
  - Use pre-channel to distribute personalized check-codes
  - Use Internet for voting – no UI, just entry-box to type in your code
  - Server decodes the candidate from the code
    - Anonymity is preserved thanks to homomorphic encrytion

Softer version of integrity protection

- Norwegian protocol
  - Use pre-channel to distribute personalized check-codes
  - Use Internet for voting, point and click UI
  - Server replies with check-code over post-channel
    - Anonymity is preserved thanks to homomorphic encrytion

Problems with the protocol

- Additional channels introduce new problems
  - What channels can we use?
  - Which requirements?
  - Is it organizationally feasible?
- Detection is not a proof – how to react if malicious voter claims that his ballot was tampered with

Current approach

- Monitoring the situation in Internet
- Hardened application that monitors the environment in client computer and protects itself
- No provable security – countermethod to every method
- Novel attack-vectors go undetected

Anti reverse engineering

- How to avoid reverse engineering?
  - Obfuscation
  - Short election period
  - Weakest link shall be attacked, thus everything must be obfuscated: also protocol
  - How to detect that the protection has been broken?
  - Closed source by definition

Back to real life

- Somebody claims that virus modified his ballot
  - Check the facts
  - How widespread is it?
  - Make decision – revoke or not to revoke
- Problem must have significant influence to results in order to get results revoked
- This is not a technical matter
- Acceptable risk

?

- We talked about malicious voters, malicious NEC, malicious developers
-
- What harm could malicious cryptographer cause?

Should we take new protocol?

- Integrity protection is only one facet of the i-voting system
- New protocols must be analyzed carefully
  - How the system as a whole gets affected?
  - Is the technology capable enough?
  - Is the cost acceptable?
  - Which new attack-vectors are created?

Road ahead

- Protect the current protocol
  - Model and implement attacks
  - Model and implement protection mechanisms
- Research new protocols
  - We need cryptographers to commit
- Educate
  - Explain risks and teach how to avoid them

- I-voting is not a goal, it's just one voting method